

Cryptography

Past, Present and Future

Imad Fakhri Taha Al Shaikhli

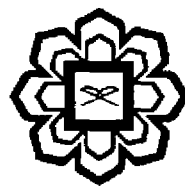


IIUM PRESS

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

Cryptography: Past, Present and Future

Imad Fakhri Taha Al Shaikhli



IIUM Press

Published by:
IIUM Press
International Islamic University Malaysia

First Edition, 2011

©IIUM Press, IIUM

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without any prior written permission of the publisher.

Perpustakaan Negara Malaysia

Cataloguing-in-Publication Data

Imad Fakhri Taha Al-Shaikhli
Cryptography: Past, Present and Future
Imad Fakhri Taha Al-Shaikhli

ISBN: 978-967-418-091-1

Member of Majlis Penerbitan Ilmiah Malaysia – MAPIM
(Malaysian Scholarly Publishing Council)

Printed by :
IIUM PRINTING SDN. BHD.
No. 1, Jalan Industri Batu Caves 1/3
Taman Perindustrian Batu Caves
Batu Caves Centre Point
68100 Batu Caves
Selangor Darul Ehsan

TABLE OF CONTENTS

Dedication	I
Preface	Vii
Acknowledgement	Viii
PART I Classical Cryptography	1
Chapter One Introduction	3-9
- Imad Fakhri Taha Al Shaikhli	
- Rusydi Hasan	
- Nurhidayah Binti Abdulrashid	
- Faizurimawaty Bt Padzilah	
- Nabilah Bt Abd Rahman	
Chapter Two Monoalphabetic Substitution Cipher	11-16
- Imad Fakhri Taha Al Shaikhli	
- Rusydi Hasan	
- Nurhidayah Binti Abdulrashid	
- Faizurimawaty Bt Padzilah	
- Nabilah Bt Abd Rahman	
Chapter Three Polyalphabetic Substitution Cipher	17-23
- Imad Fakhri Taha Al Shaikhli	
- Rusydi Hasan	
- Nurhidayah Binti Abdulrashid	
- Faizurimawaty Bt Padzilah	
- Nabilah Bt Abd Rahman	
Chapter Four Machine-Based Cryptography	25-30
- Rusydi Hasan	
- Imad Fakhri Taha Al Shaikhli	
- Nurhidayah Binti Abdulrashid	
- Faizurimawaty Bt Padzilah	
- Nabilah Bt Abd Rahman	
PART II Modern Symmetric-Key Cryptography	31
Chapter Five Block and Stream Cipher	33-38
- Sufyan Salim Mahmood Al Dabbagh	
- Imad Fakhri Taha Al Shaikhli	
- Muhammad Fadil Lubis	
- Usman bin Mohd Azhar	
- Nopan Ziro Ando	
Chapter Six Data Encryption Standard (DES)	39-46
- Imad Fakhri Taha Al Shaikhli	

<ul style="list-style-type: none"> - Sufyan Salim Mahmood Al Dabbagh - Muhammad Fadil Lubis - Usman bin Mohd Azhar - Nopan Ziro Ando 	
Chapter Seven Advanced Encryption Standard(Rijndael)	47-52
<ul style="list-style-type: none"> - Sufyan Salim Mahmood Al Dabbagh - Imad Fakhri Taha Al Shaikhli - Muhammad Fadil Lubis - Usman bin Mohd Azhar - Nopan Ziro Ando 	
Chapter Eight Trivium and Rabbit Stream Cipher	53-61
<ul style="list-style-type: none"> - Imad Fakhri Taha Al Shaikhli - Sufyan Salim Mahmood Al Dabbagh - Muhammad Fadil Lubis - Usman bin Mohd Azhar - Nopan Ziro Ando 	
PART III Hash Functions	63
Chapter Nine Introduction	65-72
<ul style="list-style-type: none"> - Khanssaa Munthir Abdulmajed - Imad Fakhri Taha Al Shaikhli - Sufyan Salim Mahmood Al Dabbagh - Ahmad Faridi Abdul Matin - Sibomana Hilali Hussein 	
Chapter Ten Message Digest (MDX) Family	73-80
<ul style="list-style-type: none"> - Imad Fakhri Taha Al Shaikhli - Sufyan Salim Mahmood Al Dabbagh - Khanssaa Munthir Abdulmajed - Ahmad Faridi Abdul Matin - Sibomana Hilali Hussein 	
Chapter Eleven SHA family hash function	81-87
<ul style="list-style-type: none"> - Khanssaa Munthir Abdulmajed - Imad Fakhri Taha Al Shaikhli - Sufyan Salim Mahmood Al Dabbagh - Ahmad Faridi Abdul Matin - Sibomana Hilali Hussein 	
Chapter Twelve RIPEMD and Chameleon Hash Function	89-96
<ul style="list-style-type: none"> - Sufyan Salim Mahmood Al Dabbagh - Imad Fakhri Taha Al Shaikhli - Khanssaa Munthir Abdulmajed - Ahmad Faridi Abdul Matin 	

- Sibomana Hilali Hussein

PARTIV Public Key & Digital Signature Schemes	97
Chapter Thirteen Rivest-Shamir-Adleman (RSA)	99-105
<ul style="list-style-type: none"> - Iqram Mohammed Hayek - Imad Fakhri Taha Al Shaikhli - Sufyan Salim Mahmood Al Dabbagh - Kusai Abu Hilal 	
Chapter Fourteen Cryptanalysis of RSA	107-112
<ul style="list-style-type: none"> - Imad Fakhri Taha Al Shaikhli - Sufyan Salim Mahmood Al Dabbagh - Iqram Mohammed Hayek - Kusai Abu Hilal 	
Chapter Fifteen Digital Signature Algorithm	113-115
<ul style="list-style-type: none"> - Sufyan Salim Mahmood Al Dabbagh - Imad Fakhri Taha Al Shaikhli - Iqram Mohammed Hayek - Kusai Abu Hilal 	
Part V Zero-Knowledge Proof	116
Chapter Sixteen Background of Zero-Knowledge Proof	117-120
<ul style="list-style-type: none"> - Imad Fakhri Taha Al Shaikhli - Rusydi Hasan - Siti Khairunnisa Mohd Bakri - Nur Dalilah Bt More Yusoff - Nur Khairunnisa Bt Juara 	
Chapter Seventeen Interactive Proof Systems	121-126
<ul style="list-style-type: none"> - Rusydi Hasan - Imad Fakhri Taha Al Shaikhli - Siti Khairunnisa Mohd Bakri - Nur Dalilah Bt More Yusoff - Nur Khairunnisa Bt Juara 	
Chapter Eighteen Zero-Knowledge Proof	127-132
<ul style="list-style-type: none"> - Imad Fakhri Taha Al Shaikhli - Rusydi Hasan 	

- Siti Khairunnisa Mohd Bakri	
- Nur Dalilah Bt More Yusoff	
- Nur Khairunnisa Bt Juara	
Chapter Nineteen Feige-Fiat-Shamir Identification Scheme	133-138
- Rusydi Hasan	
- Imad Fakhri Taha Al Shaikhli	
- Siti Khairunnisa Mohd Bakri	
- Nur Dalilah Bt More Yusoff	
- Nur Khairunnisa Bt Juara	
Part VI Secret Sharing	139
Chapter Twenty Introduction	141-146
- Muhammad Israfil	
- Imad Fakhri Taha Al Shaikhli	
- Sufyan Salim Mahmood Al Dabbagh	
Chapter Twenty One Shamir's Threshold Scheme	147-150
- Imad Fakhri Taha Al Shaikhli	
- Sufyan Salim Mahmood Al Dabbagh	
- Muhammad Israfil	
Chapter Twenty Two Blakely's Secret Sharing Scheme	151-155
- Sufyan Salim Mahmood Al Dabbagh	
- Imad Fakhri Taha Al Shaikhli	
- Muhammad Israfil	
Part VII Quantum Cryptography	156
Chapter Twenty Three Quantum Cryptography	
- Azeddine Messikh	

20. Introduction

- Muhammad Israfil
- Imad Fakhri Taha Al Shaikhli
- Sufyan Salim Mahmood Al Dabbagh

ABSTRACT

In this research paper, we would like to elaborate one of the cryptography methods to secure the information or the secret which is “Secret Sharing Scheme” that would be divided into two main parts which are: Shamir’s threshold scheme and Blakely’s secret sharing scheme. Both of these methods are using threshold scheme which is the most basic and old way to do secret sharing. Also, both of these methods are using difference approach to deliver and divide the secret to secure the fatal information. Also, we would like to discuss and share the common problem that the secret sharing would face in reality and what are the approaches to be done in order to minimize the problem so that the secret or the information is to be kept confidential.

BACKGROUND

Cryptography is one of many Medias to keep the secrecy of the information. In the past, cryptography helped ensure secrecy in important communications, such as those of spies, military leaders, and diplomats. In recent decades, the field of cryptography has expanded its remit in two ways. Firstly, it provides mechanisms for more than just keeping secrets. As example, schemes like digital signatures and digital cash. Secondly, cryptography has come to be in widespread use by many civilians who do not have extraordinary needs for secrecy, although typically it is transparently built into the infrastructure for computing and telecommunications, and users are not aware of it. Regarding this issues, there many methods to secure the